

JC17 Rec'd PCT/PTO 31 MAY 2001

FORM PTO-1390 US DEPARTMENT OF COMMERCE REV. 5-93 PATENT AND TRADEMARK OFFICE		ATTORNEYS DOCKET NUMBER P01,0183
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/857153
INTERNATIONAL APPLICATION NO. PCT/EP99/09496	INTERNATIONAL FILING DATE 04 DECEMBER 1999	PRIORITY DATE CLAIMED 04 DECEMBER 1998
TITLE OF INVENTION METHOD OF SECURE DATA TRANSMISSION		
APPLICANT(S) FOR DO/EO/US Klaus David GRADISCHNIG et al		
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:		
<p>1. <input checked="" type="checkbox"/> This is a FIRST submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371. 3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay. 4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.</p> <p>5. <input checked="" type="checkbox"/> A copy of International Application as filed (35 U.S.C. 371(c)(2)). a. <input checked="" type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> has been transmitted by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US) A translation of the International Application into English (35 U.S.C. 371(c)(2)).</p> <p>6. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3)) a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> have been transmitted by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input checked="" type="checkbox"/> have not been made and will not be made.</p> <p>7. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</p> <p>8. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).</p> <p>9. <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).</p> <p>10. <input type="checkbox"/> Items 11. to 16. below concern other document(s) or information included:</p> <p>11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; (PTO 1449, Prior Art, Search Report, 05 References).</p> <p>12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. (SEE ATTACHED ENVELOPE)</p> <p>13. <input checked="" type="checkbox"/> Amendment "A" Prior to Action and Appendix "A". <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment.</p> <p>14. <input checked="" type="checkbox"/> A substitute specification and substitute specification mark-up.</p> <p>15. <input checked="" type="checkbox"/> A change of address letter attached to the Declaration.</p> <p>16. <input checked="" type="checkbox"/> Other items or information: a. <input checked="" type="checkbox"/> Submission of Drawings and drawing changes b. <input checked="" type="checkbox"/> Appointment of Associate Power of Attorney c. <input checked="" type="checkbox"/> EXPRESS MAIL #EL 843728230 US dated May 31, 2001</p>		

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO PCT/EP99/09496	ATTORNEYS DOCKET NUMBER P01,0183		
17. <input checked="" type="checkbox"/> The following fees are submitted:		CALCULATIONS		
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO \$860.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) \$690.00 No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)) \$710.00 Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO \$1000.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$ 100.00		PTO USE ONLY		
ENTER APPROPRIATE BASIC FEE AMOUNT =		\$ 860.00		
Surcharge of \$130.00 for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).		\$		
Claims	Number Filed	Number Extra	Rate	
Total Claims	04 - 20 =	0	X \$ 18.00	\$
Independent Claims	04 - 3 =	1	X \$ 80.00	\$ 80.00
Multiple Dependent Claims		\$270.00 +	\$	
TOTAL OF ABOVE CALCULATIONS =		\$ 940.00		
Reduction by 1/2 for filing by small entity, if applicable Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)		\$		
SUBTOTAL =		\$ 940.00		
Processing fee of \$130.00 for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)) +		\$		
TOTAL NATIONAL FEE =		\$ 940.00		
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property +				
TOTAL FEES ENCLOSED =		\$ 940.00		
		Amount to be refunded	\$	
		charged	\$	
a. <input checked="" type="checkbox"/> A check in the amount of <u>\$ 940.00</u> to cover the above fees is enclosed. b. <input type="checkbox"/> Please charge my Deposit Account No. _____ in the amount of \$ _____ to cover the above fees. A duplicate copy of this sheet is enclosed. c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>50-1519</u> . A duplicate copy of this sheet is enclosed. NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.				
<u>SEND ALL CORRESPONDENCE TO:</u>				
SCHIFF HARDIN & WAITE PATENT DEPARTMENT 6600 Sears Tower 233 South Wacker Drive Chicago, Illinois 60606-6473		<u>Mark Bergner</u> SIGNATURE MARK BERGNER (REG. NO. 45,877)		
DATE: May 31, 2001				
CUSTOMER NUMBER 26574				

SPECIFICATION

TITLE

METHOD OF SECURE DATA TRANSMISSION

BACKGROUND OF THE INVENTION

5 Field of the Invention

[0001] The invention relates to a method of transmitting data securely in which redundant messages are transmitted.

Description of the Related Art

[0002] Many transmission media/protocols have a transmit-receive property in which messages transferred to a medium by the transmitter arrive at the receiver in the same way (assuming that they arrive at all) that they were transmitted. In other words, message overhaul does not take place. Many protocols ensuring secure message transmission have this transmit-receive property as a prerequisite for the underlying transmission media/protocols which they use, since this transmit-receive property makes it much simpler to ensure efficient, secure message transmission.

10 Historically, there has been a problem of defining protocols for secure message transmission which do not require this transmit-receive property (i.e., possibly having message overhaul).

[0003] The following methods are (or may be) used for the purpose of defining such protocols. Although a prerequisite of the MTP standard (cf. Q.700 to Q.706) involves transmission media on which message overhaul cannot take place, MTP Level 2 (Q.703) is also able to operate with transmission media which do not have the transmit-receive property.

[0004] It is fundamental to the operation of the protocol (Basic Error Correction), even in the case of message overhaul, that the MTP recognizes after a retransmission request whether a particular message has been sent on the basis of the retransmission request (it is then accepted), or whether it was actually sent before the retransmission request (it is then discarded). However, a disadvantage of this protocol is that it has no selective retransmission mode, which can be inefficient.

In addition, without modification of MTP Level 2, the entire available bandwidth would be used, which may be disadvantageous.

[0005] MTP Level 2 with the Preventive Cyclic Retransmission method can also operate with message overhaul, since no retransmission requests are generated and messages which do not arrive in the correct order are discarded.

5 Again, the disadvantage of the method is a poor utilization of the bandwidth.

[0006] TCP, which uses IP as underlying network protocol, has also solved the problem. Transmitted blocks which are not acknowledged are retransmitted when a timer has run out. This protocol mechanism (in which only blocks received without gaps are acknowledged) results in unnecessary retransmissions, depending on the round trip delay (even if the acknowledgement timeout is chosen to be long enough) since the acknowledgement timer often also runs out for messages which have been received correctly after a lost message.

10 [0007] The situation is improved somewhat by methods such as Fast Retransmission and providing an explicit NACK upon the first occurrence of a gap.

15 [0008] The Reliable Data protocol works in a similar way to TCP, with the extension that messages which are not received without gaps can also be acknowledged.

SUMMARY OF THE INVENTION

20 [0009] The present invention extends and modifies certain existing protocols in order to ensure efficient, secure data transmission using transmission media and protocols in which message overhaul can take place.

[0010] In this context, the present invention is based on the realization that, for a modern protocol which is intended to work efficiently (i.e., more rapidly) using a 25 transmission medium/protocol with possible message overhaul, and having loss detection with minimization of unnecessarily transmitted information, the following properties are advantageous:

- a) multiple selective retransmission method without full dependency on a timer; specifically, the loss of an ACK should not result in retransmission,

30

5

- b) explicit status alignment between a transmitter and receiver,
- c) retransmission of a message only if there is a certain probability that the message is lost,
- d) messages received a plurality of times must not cause an incorrect response, and
- e) use of parameter value selection to determine the tradeoff between rapid error correction and minimum unnecessary message transmission.

10 [0011] The most important of these points is point (d). Specifically, there are two opportunities/situations for messages received more than once to cause incorrect responses:

15

- i) the message is recognized as having already been received, and this is defined as an error in accordance with the protocol; and
- ii) the message is interpreted as a new message and triggers an action which later results in an error being detected in a transmitter or receiver as a consequence. By way of example, a supposed message loss may be detected by virtue of such a message. This results in a retransmission request for messages which have not actually been sent yet, which is interpreted as an error by the transmitter.

20 [0012] One option for guaranteeing item (d) in protocols which satisfy the other items sufficiently, but not item (d), is for a message transmitted for the second time or more to be specially marked. Such protocols can then easily be changed so that such marked messages are simply ignored in the situations described under (i) and (ii).

25 [0013] Another opportunity to eliminate situation (i) is to ignore such messages as a general rule.

[0014] For situation (ii), a window can also be defined so that messages received outside of this window are generally ignored and do not result in any retransmission requests.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Exemplary embodiments of the invention are explained in more detail with the aid of figures.

5 Figure 1 is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 3 of the ITU-T Recommendation Q.2110;

10 Figure 2 is a data structure diagram showing the structure of the Poll Protocol Data Unit (SD-PDU) according to prior art Figure 4 of the ITU-T Recommendation Q.2110;

15 Figure 3 is a data structure diagram showing the structure of the Sequenced Data Protocol Data Unit (SD-PDU) according to prior art Figure 5 of the ITU-T Recommendation Q.2110;

20 Figures 4A & 4B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;

25 Figures 5A & 5B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 43 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;

30 Figures 6A & 6B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 44 of 51, of the ITU-T Recommendation Q.2110 as modified by method 1 of the present invention;

35 Figures 7A & 7B are flowchart segments showing the SSCOP processing according to Figure 20, sheet 40 of 51, of the ITU-T Recommendation Q.2110 as modified by method 2 of the present invention; and

40 Figure 8 is a flowchart segments showing the SSCOP processing according to common elements of Figure 20, from sheets 40, 41, 43 and 44 of 51, of the ITU-T Recommendation Q.2110.

DETAILED DESCRIPTION OF THE INVENTION

[0016] The exemplary embodiment chosen is the protocol Service Specific Connection-Oriented Protocol (SSCOP) described in ITU-T Recommendation Q.2110 (07/94) - B-ISDN ATM ADAPTATION LAYER - SERVICE SPECIFIC

5 CONNECTION ORIENTED PROTOCOL (SSCOP) Q.2110 (herein incorporated by reference). This protocol fulfills the properties (a) through (c) identified above, but has the problems described under (i) and (ii). Specifically, when the message is recognized as having already been received and this is defined as an error in accordance with the protocol (i), this results in an incorrect response (branch to the 10 connector D) in ITU-T Rec. Q.2110 (Figure 4B). Similarly, Figures 4A and 4B show that a message having the property described in (ii) usually results in a retransmission request (USTAT). This in turn usually results in a branch to the error branch (connector D) in Figure 5B.

[0017] In one embodiment of the invention, method 1, in accordance with the 15 discussion above, a Sequenced Data Protocol Data Unit (SD-PDU) is now specially marked in the case of repeated transmission, e.g., by setting bit 5 in the PDU trailer (Figure 1, the RX field) to 1 (Figure 5A, 5.1), indicating a repeated transmission. This embodiment modifies the ITU-T Rec. Q.2110, Figure 20 (sheet 40 of 51) such that, in the two error situations described above, a check is first carried out to 20 determine whether the SD-PDU is marked as having been repeated (Figure 4A, 4.1). In this case, the message is ignored and an incorrect response cannot occur.

[0018] Alternatively, in method 2, the ITU-T Rec. Q.2110 figure 20 (sheet 40 of 51) is modified such that the error case (i) is generally not checked, and a 25 message which has already been received is simply ignored (Figure 7B, 7.2, TRUE path). In addition, likewise in Figure 7A, the ITU-T Rec. Q.2110 figure 20 (sheet 40 of 51) is modified such that, after the query $VR(H) < VR(MR)$, a check is carried out to determine whether $SD.N(S) < VR(R) + 2^{23}$, for example (Figure 7B, 7.2). (This presupposes that the window size used for the flow control is always smaller than 2^{23} , which does not represent any relevant restriction, however). If this is not the 30 case, the message is discarded (Figure 7A, 7.1, FALSE path), otherwise it is handled as previously.

[0019] Item (e) can also easily be achieved with SSCOP, e.g., USTATs could be sent only with a certain time delay, in order to wait for messages which have

been repeated. In addition, it would be possible for only gaps which have already existed for a certain time to be reported (or heeded) using/in the case of a STAT.

[0020] The above-described methods are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

ABSTRACT

[0021] The invention shows how certain existing protocols can be enlarged/modified in order to guarantee an efficient, secure data transmission via transmission media/protocols, whereby message overhaul can occur. The invention 5 relates to a method by way of which a message, which has been transmitted for at least the second time, is particularly marked by the transmitter. The message which is marked as transmitted for at least the second time is ignored by the receiver when the message has already been received or is new.

5 BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

10 **PRELIMINARY AMENDMENT A**
PRIOR TO ACTION

APPLICANT(S): Klaus David GRADISCHNIG et al
ATTORNEY DOCKET NO.: P01,0183
INTERNATIONAL APPLICATION NO: PCT/EP99/09496
INTERNATIONAL FILING DATE: 04 December 1999
INVENTION: METHOD OF SECURE DATA TRANSMISSION

15 Assistant Commissioner for Patents,
Washington D.C. 20231

10 Sir:

Applicants herewith amend the above-referenced PCT application, and
request entry of the Amendment prior to examination on the United States
Examination Phase.

15 **IN THE CLAIMS:**

On page 6:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-4 with the following rewritten claims 1-4,
referring to the mark-ups in Appendix A.

20 1. (Amended) A method of secure data transmission which is executed on a
layer basis using a transmission method having possible message overhaul,
comprising the steps of:

25 specially marking a message which is already being transmitted for at least a
second time by said transmitter; and

ignoring said message which is marked as having been transmitted for at
least a second time by a receiver if it recognizes said message as having already
been received or if it interprets said message as a new message.

2. (Amended) A method of secure data transmission wherein a transmitter protocol operates on a layer basis using a transmitter protocol having possible message overhaul, comprising the steps of:

5 specially marking, by said transmitter protocol, a message which is already being transmitted for at least a second time.

3. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

10 ignoring, by said receiver protocol, a message which is marked as having been transmitted at least for a second time if it recognizes the message as having already been received or if it interprets said message as a new message.

15 4. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

ignoring, by said receiver protocol, a message if it recognizes said message as having already been received or if, although it interprets said message as a new message, said message is situated outside of a prescribed window.

20 **REMARKS**
The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

5

(Reg. No. 45,877)

Mark Bergner
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
(312) 258-5779
Attorneys for Applicant

10

15

CUSTOMER NUMBER 26574

He was a man of great energy and a strong leader, and he left a lasting mark on the field of education.

Appendix A
Mark Ups for Claim Amendments

1. (Amended) A method of secure data transmission which is executed on a
5 layer basis using a transmission method [with]having possible message overhaul,
comprising the steps of:
[characterized in that]
[a]-specially marking a message which is already being transmitted for at
least [the]a second time [is specially marked] by [the]said transmitter[.]; and
10 [b) — a]ignoring said message which is marked as having been transmitted
for at least [the]a second time [is ignored] by [the]a receiver if it recognizes [the]said
message as having already been received or if it interprets [the]said message as a
new message.

15 2. [-A] (Amended) A method of secure data transmission wherein a
transmitter protocol[-which] operates on a layer basis using a transmitter protocol
[with]having possible message overhaul, comprising the steps of:
[characterized in that]
[it]specially [marks]marking, by said transmitter protocol, a message
20 which is already being transmitted for at least [the]a second time.

25 3. [-A] (Amended) A method of secure data transmission wherein a
receiver protocol[-which] operates on a layer basis using a receiver protocol
[with]having possible message overhaul, comprising the steps of:
[characterized in that]
[it ignores]ignoring, by said receiver protocol, a message which is marked
as having been transmitted at least for [the]a second time if it recognizes the
message as having already been received or if it interprets [the]said message as a
new message.

30 4. [-A] (Amended) A method of secure data transmission wherein a
receiver protocol[-which] operates on a layer basis using a receiver protocol
[with]having possible message overhaul, comprising the steps of:
[characterized in that]

[it ignores]ignoring, by said receiver protocol, a message if it recognizes [the]said message as having already been received or if, although it interprets [the]said message as a new message, [this]said message is situated outside of a prescribed window.

5

Document comparison done by DeltaView on Wednesday, May 09, 2001 10:11:19

Input:	
Document 1	file:///Q:\documents\Year 2001\p010183-gradsechnig-secure data transmission\original claims.doc
Document 2	file:///Q:\documents\Year 2001\p010183-gradsechnig-secure data transmission\amended claims.doc
Rendering set	Mark PTO

Legend:	
Insertion	
[Deletion]	
[Moved from]	
Moved to	
Format change	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:		
	Count	% of content
Insertions	31	25.16%
Deletions	35	12.03%
Moves	0	0.00%
Matched	32	62.81%
Format changed	0	0.00%

10

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

REQUEST FOR APPROVAL OF DRAWING CHANGES

APPLICANT(S): Klaus David GRADISCHNIG et al
ATTORNEY DOCKET NO.: P01,0183
INTERNATIONAL APPLICATION NO: PCT/EP99/09496
INTERNATIONAL FILING DATE: 04 December 1999
INVENTION: METHOD OF SECURE DATA TRANSMISSION

Assistant Commissioner for Patents,
Washington, D.C. 20231

Sir:

Enclosed are eleven sheets of drawings showing in red, changes to the Figures. Approval of the changes is respectfully requested.

Submitted by,

(Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
Chicago, Illinois 60606-6473
(312) 258-5779
Attorney for Applicant(s)

CUSTOMER NUMBER 26574

532 Rec'd PCT/US 31 MAY 2001

BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

5

PRELIMINARY AMENDMENT A
PRIOR TO ACTION

APPLICANT(S): Klaus David GRADISCHNIG et al
ATTORNEY DOCKET NO.: P01,0183
INTERNATIONAL APPLICATION NO: PCT/EP99/09496
INTERNATIONAL FILING DATE: 04 December 1999
INVENTION: METHOD OF SECURE DATA TRANSMISSION

10 Assistant Commissioner for Patents,
Washington D.C. 20231

15 Sir:

Applicants herewith amend the above-referenced PCT application, and
request entry of the Amendment prior to examination on the United States
Examination Phase.

15

IN THE CLAIMS:

20 On page 6:

replace line 1 with --WHAT IS CLAIMED IS:--;

25 Please replace original claims 1-4 with the following rewritten claims 1-4,
referring to the mark-ups in Appendix A.

20

1. (Amended) A method of secure data transmission which is executed on a
layer basis using a transmission method having possible message overhaul,
comprising the steps of:

25 specially marking a message which is already being transmitted for at least a
second time by said transmitter; and

ignoring said message which is marked as having been transmitted for at
least a second time by a receiver if it recognizes said message as having already
been received or if it interprets said message as a new message.

2. (Amended) A method of secure data transmission wherein a transmitter protocol operates on a layer basis using a transmitter protocol having possible message overhaul, comprising the steps of:

5 specially marking, by said transmitter protocol, a message which is already being transmitted for at least a second time.

3. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

10 ignoring, by said receiver protocol, a message which is marked as having been transmitted at least for a second time if it recognizes the message as having already been received or if it interprets said message as a new message.

15 4. (Amended) A method of secure data transmission wherein a receiver protocol operates on a layer basis using a receiver protocol having possible message overhaul, comprising the steps of:

ignoring, by said receiver protocol, a message if it recognizes said message as having already been received or if, although it interprets said message as a new message, said message is situated outside of a prescribed window.

20 **REMARKS**

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

5 Mark Bergner (Reg. No. 45,877)
Mark Bergner
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
(312) 258-5779
10 Attorneys for Applicant

CUSTOMER NUMBER 26574

the *Journal of the Royal Society of Medicine* (1980, 73, 101-102) and the *Journal of Clinical Pathology* (1980, 34, 101-102).

Appendix A
Mark Ups for Claim Amendments

1. **(Amended)** A method of secure data transmission which is executed on a
5 layer basis using a transmission method [with]**having** possible message overhaul,

comprising the steps of:

[characterized in that]

[a)]**specially marking** a message which is already being transmitted for at least [the]**a** second time [is specially marked] by [the]**said** transmitter[.]; **and**

10 [b)]**ignoring said** message which is marked as having been transmitted for at least [the]**a** second time [is ignored] by [the]**a** receiver if it recognizes [the]**said** message as having already been received or if it interprets [the]**said** message as a new message.

15 2.[-A] **(Amended)** A method of secure data transmission wherein a transmitter protocol[which] operates on a layer basis using a transmitter protocol [with]**having** possible message overhaul, **comprising the steps of:**

[characterized in that]

20 [it-]specially [marks]**marking, by said transmitter protocol**, a message which is already being transmitted for at least [the]**a** second time.

25 3.[-A] **(Amended)** A method of secure data transmission wherein a receiver protocol[which] operates on a layer basis using a receiver protocol [with]**having** possible message overhaul, **comprising the steps of:**

[characterized in that]

[it ignores]**ignoring, by said receiver protocol**, a message which is marked as having been transmitted at least for [the]**a** second time if it recognizes the message as having already been received or if it interprets [the]**said** message as a new message.

30

4.[-A] **(Amended)** A method of secure data transmission wherein a receiver protocol[which] operates on a layer basis using a receiver protocol [with]**having** possible message overhaul, **comprising the steps of:**
[characterized in that]

[it ignores]ignoring, by said receiver protocol, a message if it recognizes [the]said message as having already been received or if, although it interprets [the]said message as a new message, [this]said message is situated outside of a prescribed window.

5

Page 5 of 5
Preliminary Amendment A

Description

Method of secure data transmission

5 1. What technical problem is intended to be solved by
your invention?
2. How has this problem been solved up until now?
3. In what way does your invention solve the
specified technical problem?
10 4. Exemplary embodiment(s) of the invention.

1. Many transmission media/protocols have the
property that messages transferred to the medium by the
transmitter arrive at the receiver in the same way
15 (assuming that they arrive) in which they were
transmitted. In other words, message overhaul does not
take place. Many protocols ensuring secure message
transmission have this property as a prerequisite for
the underlying transmission media/protocols which they
20 use, since this property makes it much simpler to
ensure efficient, secure message transmission. The
problem now is that of defining protocols for secure
message transmission which do not require this
property.

25 2. The following methods are used for this purpose or
may be used for this purpose: although a prerequisite
of the MTP standard (cf. Q.700 to Q.706) is
transmission media on which message overhaul cannot
30 take place, MTP Level 2 (Q.703) is also able to operate
with transmission media which do not have this
property. It is fundamental to the operation of the
protocol (Basic Error Correction), even in the case of
35 message overhaul, that the MTP recognizes after a
retransmission request whether a particular message has
been sent on the basis of the retransmission request
(it is then accepted), or whether it was actually

sent before the retransmission request (it is then discarded). However, a disadvantage of this protocol is that it has no selective retransmission mode, which can be inefficient. In addition, without modification of 5 MTP Level 2, the entire available bandwidth would be used, which may be disadvantageous.

10 MTP Level 2 with Preventive Cyclic Retransmission method can also operate with message overhaul, since no retransmission requests are generated and messages which do not arrive in the correct order are discarded. The disadvantage of the method is again poor utilization of the bandwidth.

15 TCP, which uses IP as underlying network protocol, has also solved the problem. Transmitted blocks which are not acknowledged are retransmitted when a timer has run out. The protocol mechanism (only blocks received without gaps acknowledged) results in unnecessary 20 retransmissions, depending on the round trip delay, even if the acknowledgement timeout is chosen to be long enough, since the acknowledgement timer often also runs out for messages which have been received correctly after a lost message.

25 The situation is improved somewhat by methods such as Fast Retransmission and explicit NACK upon the first occurrence of a gap.

30 The Reliable Data protocol works in a similar way to TCP, with the extension that messages which are not received without gaps can also be acknowledged.

35 3. The present invention discloses how certain existing protocols can be extended/modified in order to ensure efficient, secure data transmission using transmission media/protocols in which message overhaul can take place.

In this context, the present invention is based on the realization that, for a modern protocol which is intended to work efficiently, i.e. more rapidly, using a transmission medium/protocol with possible message 5 overhaul [lacuna] loss detection with minimization of unnecessarily transmitted information, the following properties are advantageous:

- a) multiple selective retransmission method without full dependency on a timer; specifically, the loss of 10 an ACK should not result in retransmission,
- b) explicit status alignment between transmitter and receiver,
- c) retransmission of a message only if there is a certain probability that the message is lost,
- 15 d) messages received a plurality of times must not cause an incorrect response,
- e) it should be possible to use parameter value selection to determine the tradeoff between rapid error correction and minimum unnecessary message 20 transmission.

The most important of these points is point d). Specifically, there are two opportunities for messages received more than once to cause incorrect responses:

- 25 i) the message is recognized as having already been received, and this is defined as an error in accordance with the protocol
- ii) the message is interpreted as a new message and triggers an action which later results in an error
- 30 being detected in a transmitter or receiver as a consequence. By way of example, a supposed message loss may be detected by virtue of such a message. This results in a retransmission request for messages which have not actually been sent yet, which is interpreted as an error by the transmitter.

One option for guaranteeing item d) in protocols which satisfy the other items sufficiently, but not item d),

is for a message transmitted for the second time or
more to be specially marked. Such

protocols can then easily be changed so that such messages are simply ignored in the situations described under i) and ii).

5 Another opportunity to eliminate situation i) is to ignore such messages as a general rule.

For ii), a window could also be defined, so that messages received outside of this window are generally ignored and do not result in any retransmission

10 requests.

4. The exemplary embodiment chosen is the protocol (SSCOP) described in Q.2110. This protocol fulfills the properties 3a, 3b and 3c, but has the problems 15 described under 3i) and 3ii). Specifically, 3i) results in an incorrect response (branch to the connector D) in Q.2110, figure 20 (sheet 40 of 51). Similarly, figure 20 (sheet 40 of 51) in Q.2110 shows that a message having the property presupposed in 3ii) usually results 20 in a retransmission request (USTAT). This in turn usually results in a branch to the error branch (connector D) in figure 20 (sheet 43 of 51).

In one embodiment of the invention, in accordance with 25 3), an SD-PDU is now specially marked in the case of repeated transmission, e.g. by setting bit 5 in the PDU trailer (cf. figure 3/Q.2110) to 1. Figure 20 (sheet 40 of 51) in Q.2110 is modified such that, in the two error situations described above, a check is first 30 carried out to determine whether the SD-PDU is marked as having been repeated. In this case, the message is ignored and an incorrect response cannot occur.

35 Alternatively, figure 20 (sheet 40 of 51) in Q.2110 is modified such that the error case 3i) is generally not checked, and a message which has already been received is simply ignored. In addition, likewise in figure 20 (sheet 40 of 51),

after the query $VR(H) < VR(MR)$, a check is carried out to determine whether $SD.N(S) < VR(R) + 2^{**23}$, for example. (This presupposes that the window size used for the flow control is always smaller than 2^{**23} ,
5 which does not represent any relevant restriction, however). If this is not the case, the message is discarded, otherwise it is handled as previously.

Item e) can also easily be achieved with SSCOP, e.g.
10 USTATs could be sent only with a certain time delay, in order to wait for messages which have been repeated. In addition, it would be possible for only gaps which have already existed for a certain time to be reported (or heeded) using/in the case of a STAT.

15

Patent Claims

1. A method of secure data transmission which is executed on a layer basis using a transmission method with possible message overhaul,
 - 5 characterized in that
 - a) a message which is already being transmitted for at least the second time is specially marked by the transmitter,
 - 10 b) a message which is marked as having been transmitted for at least the second time is ignored by the receiver if it recognizes the message as having already been received or if it interprets the message as a new message.
 - 15 2. A transmitter protocol which operates on a layer basis using a transmitter protocol with possible message overhaul,
 - characterized in that
 - 20 it specially marks a message which is already being transmitted for at least the second time.
 - 25 3. A receiver protocol which operates on a layer basis using a receiver protocol with possible message overhaul,
 - characterized in that
 - it ignores a message which is marked as having been transmitted at least for the second time if it recognizes the message as having already been received
 - 30 or if it interprets the message as a new message.

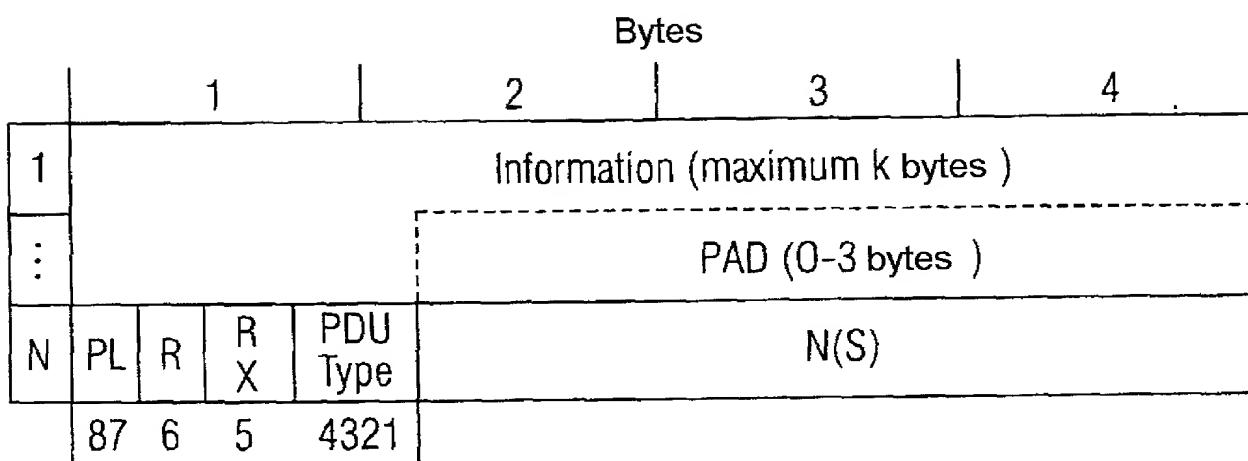
4. A receiver protocol which operates on a layer basis using a receiver protocol with possible message overhaul,
characterized in that
5. it ignores a message if it recognizes the message as having already been received or if, although it interprets the message as a new message, this message is situated outside of a prescribed window.

98 P 5890 DE

Abstract

The inventions shows how certain existing protocols can be enlarged/modified in order to guarantee an efficient, secure data transmission via transmission media/protocols, whereby message overhaul can occur.

The invention relates to a method by means of which a message, which has been transmitted for at least the second time, is particularly marked by the transmitter. The message which is marked as transmitted for at least the second time is ignored by the receiver when said message has already been received or is new.

FIG 1
Method 1

R - Reserved

RX - Retransmission indication

FIGURE 3/Q.2110
Sequenced Data PDU (SD PDU)

2/11

FIG 2

	Bytes			
	1	2	3	4
1	Reserved		N(PS)	
2	Reserved	PDU Type	N(S)	
	8765	4321		

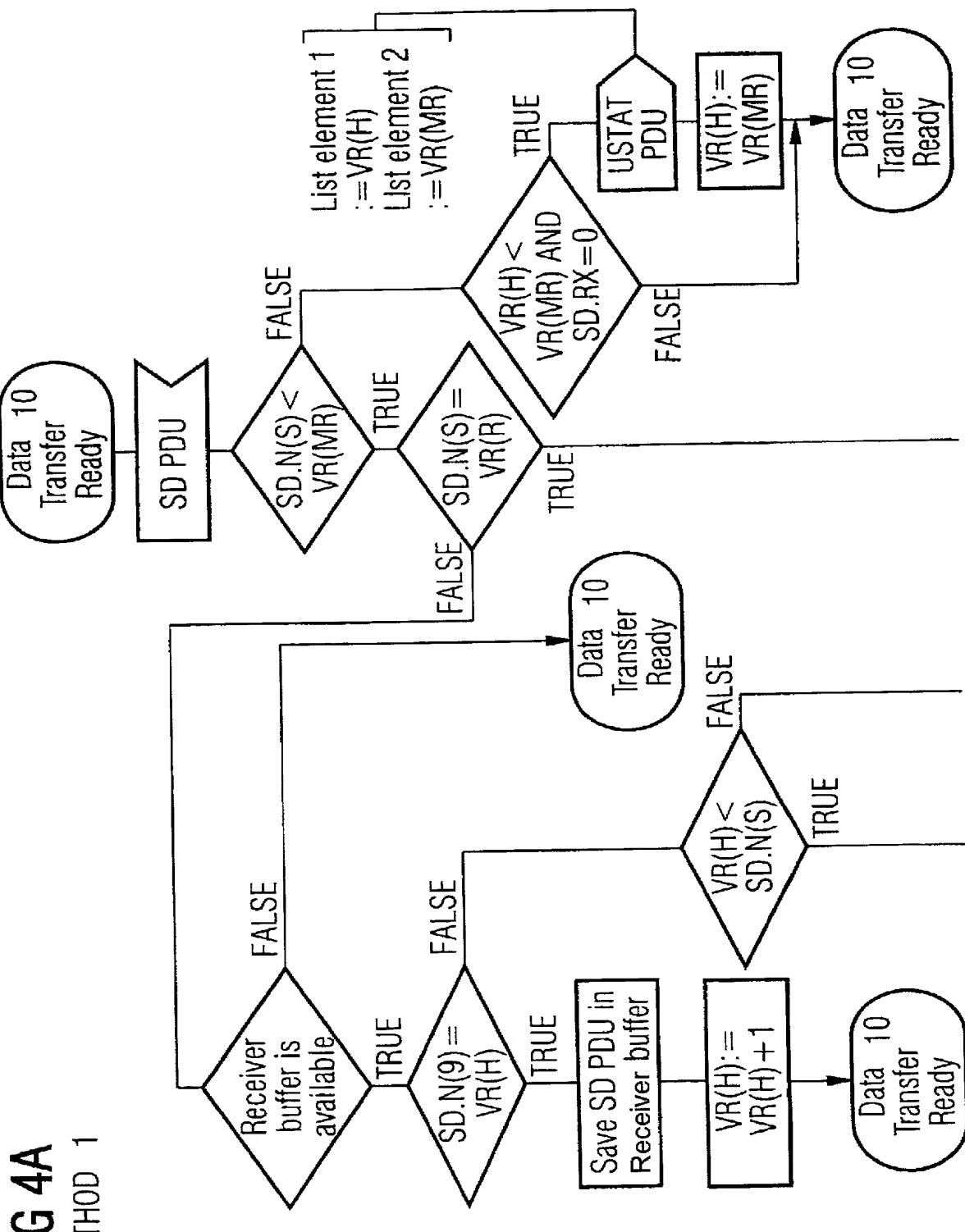
FIGURE 4/Q.2110
Poll PDU (POLL PDU)

FIG 3

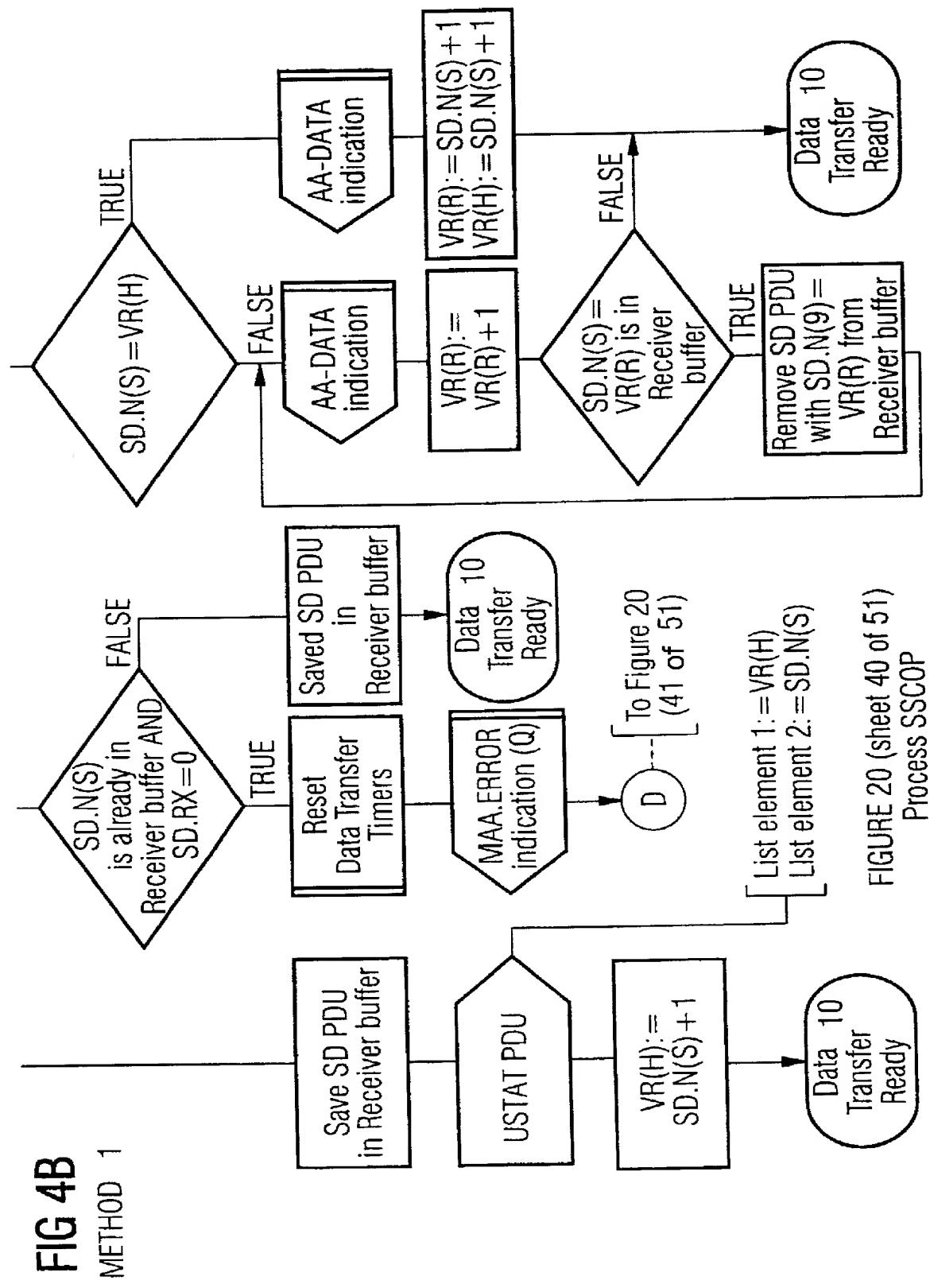
	Bytes			
	1	2	3	4
1	PAD		List element 1 (a SD PDU N(S))	
2	PAD		List element 2	
:	:		:	
L	PAD		List element L	
L+1	Rsvd		N(PS)	
L+2	Rsvd		N(MR)	
L+3	Reserved	PDU Type	N(R)	
	8765	4321		

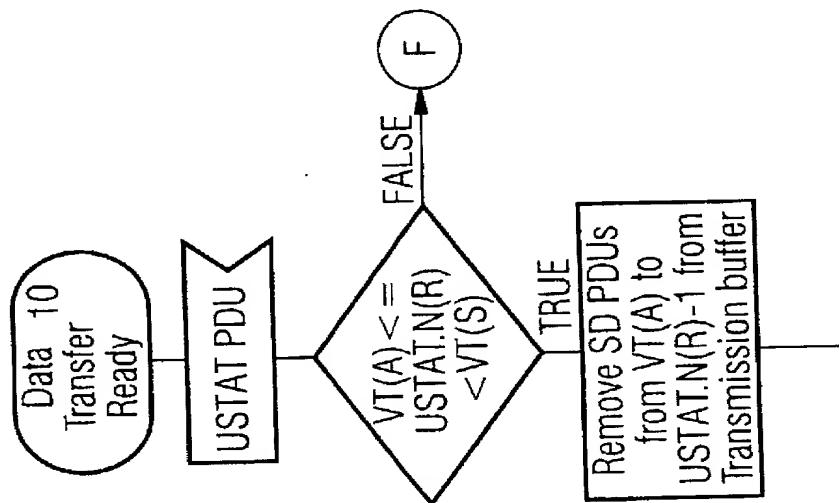
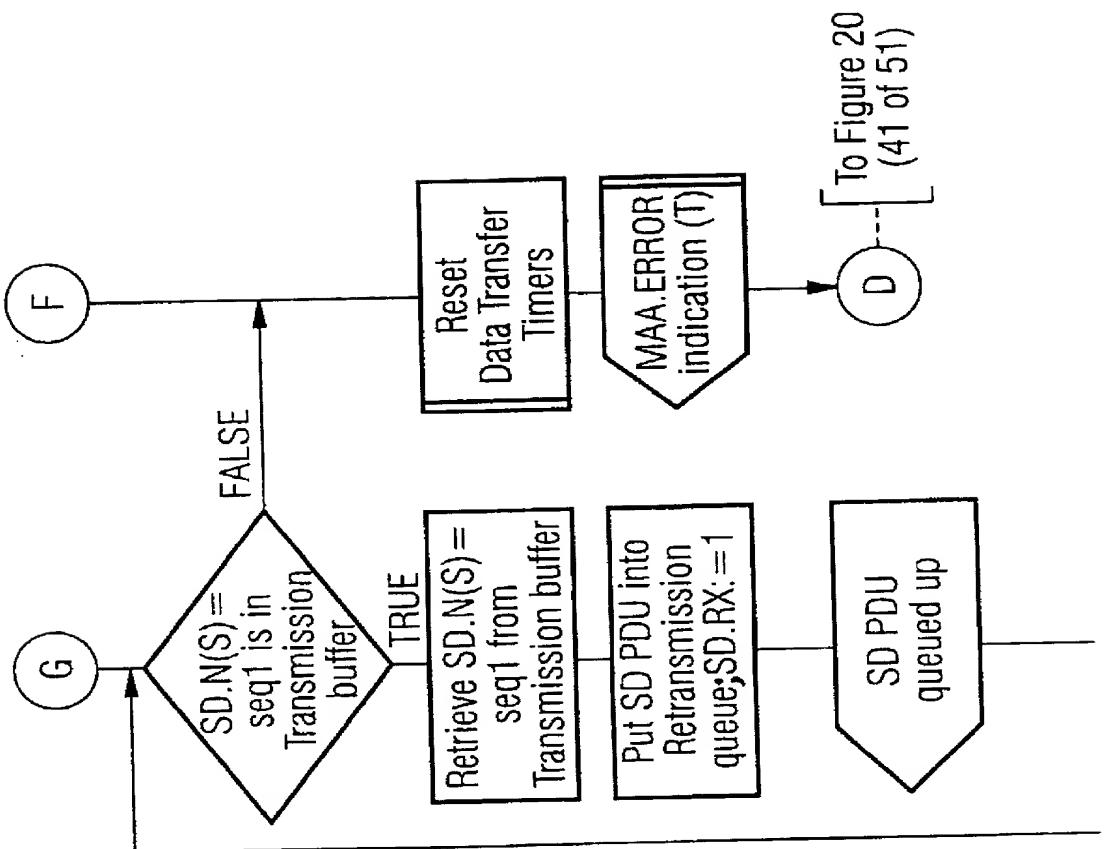
FIGURE 5/Q.2110
Solicited status PDU (STAT PDU)

3/11



4/11





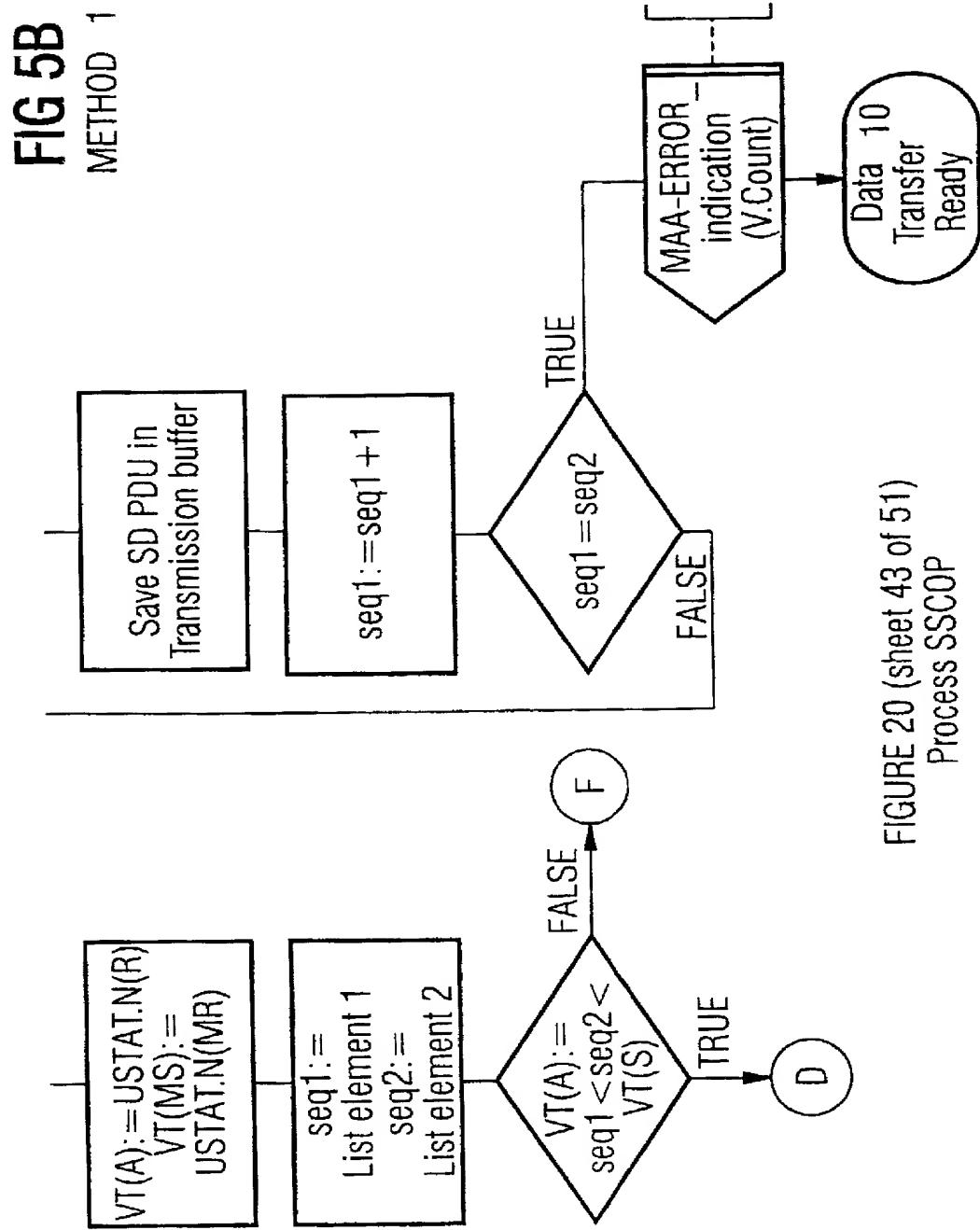


FIGURE 20 (sheet 43 of 51)
Process SSCOP

7/11

FIG 6A

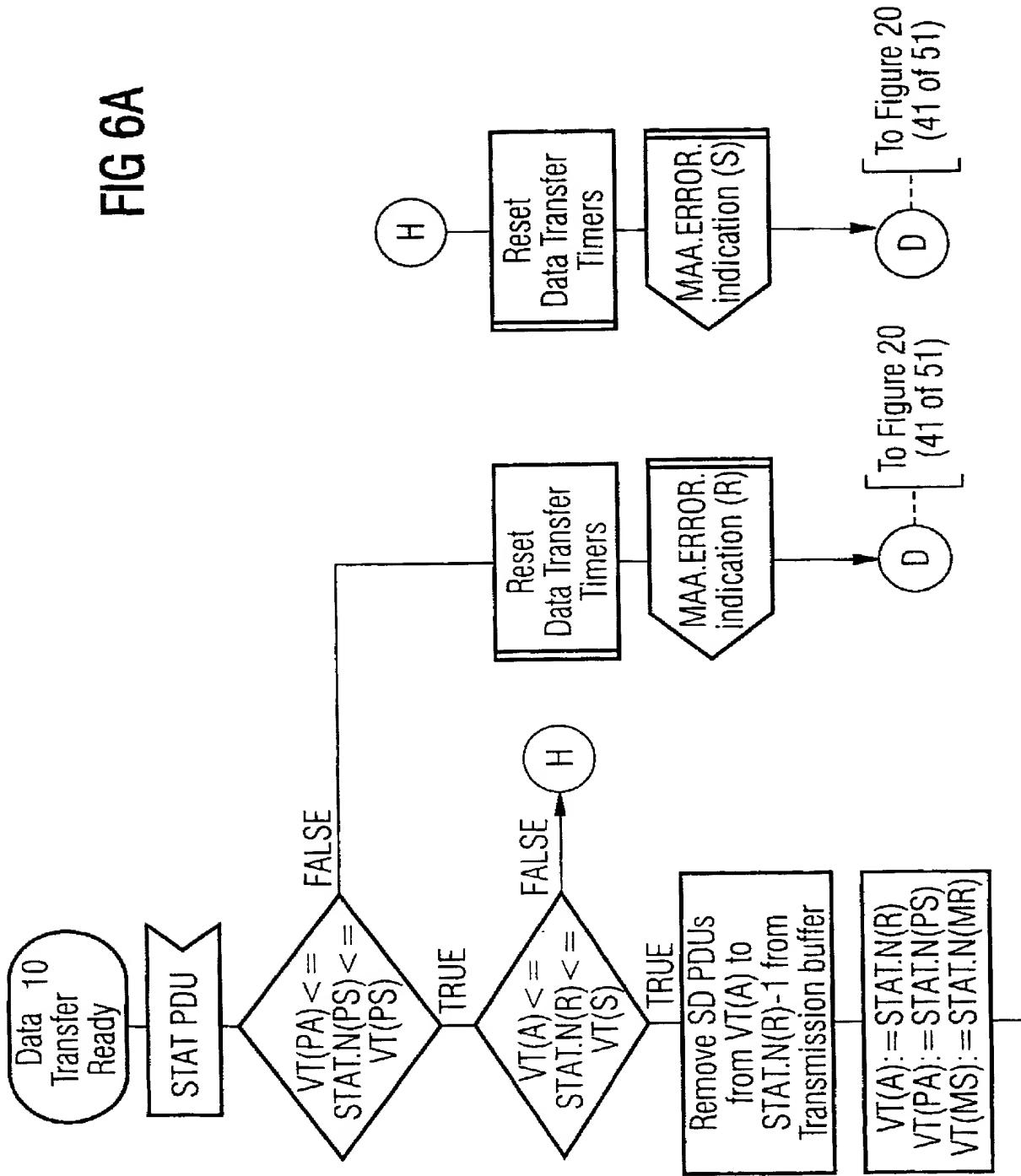


FIG 6B

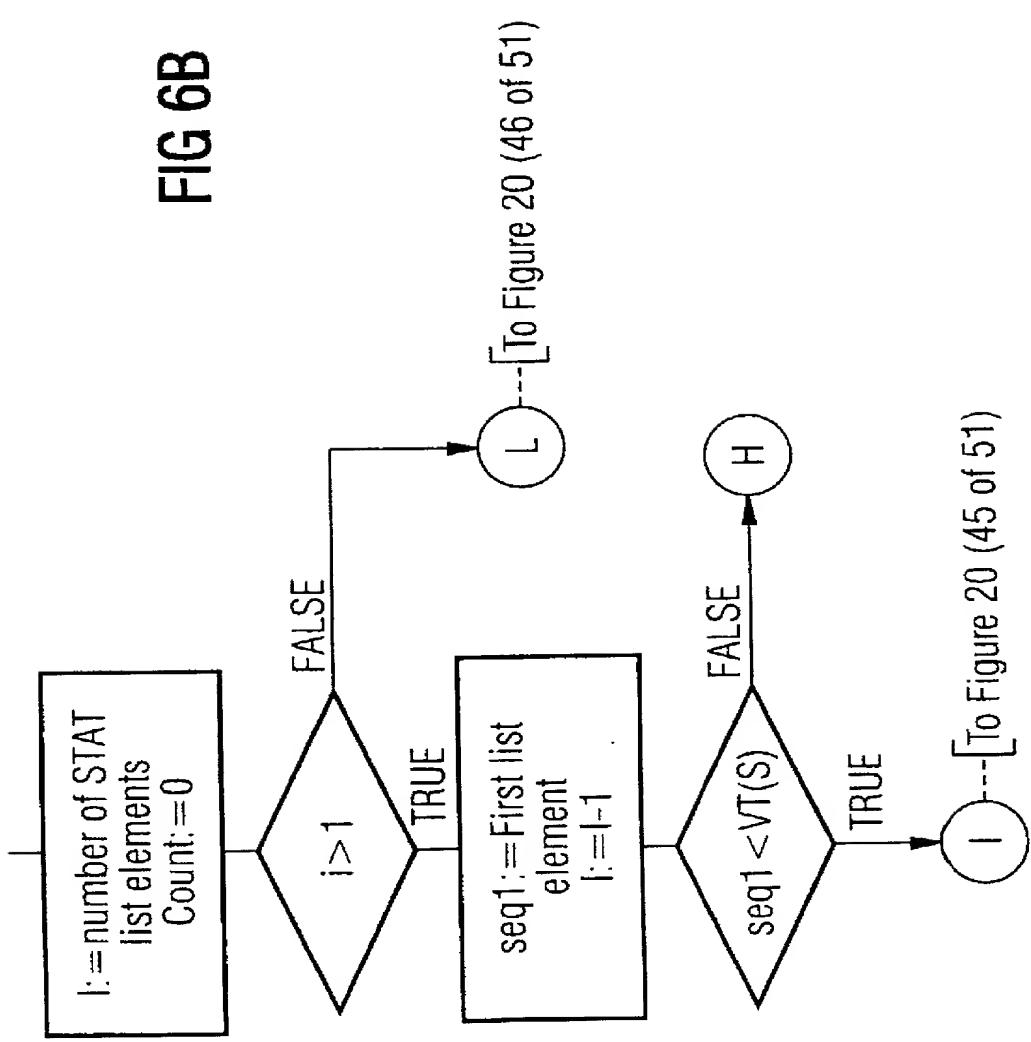
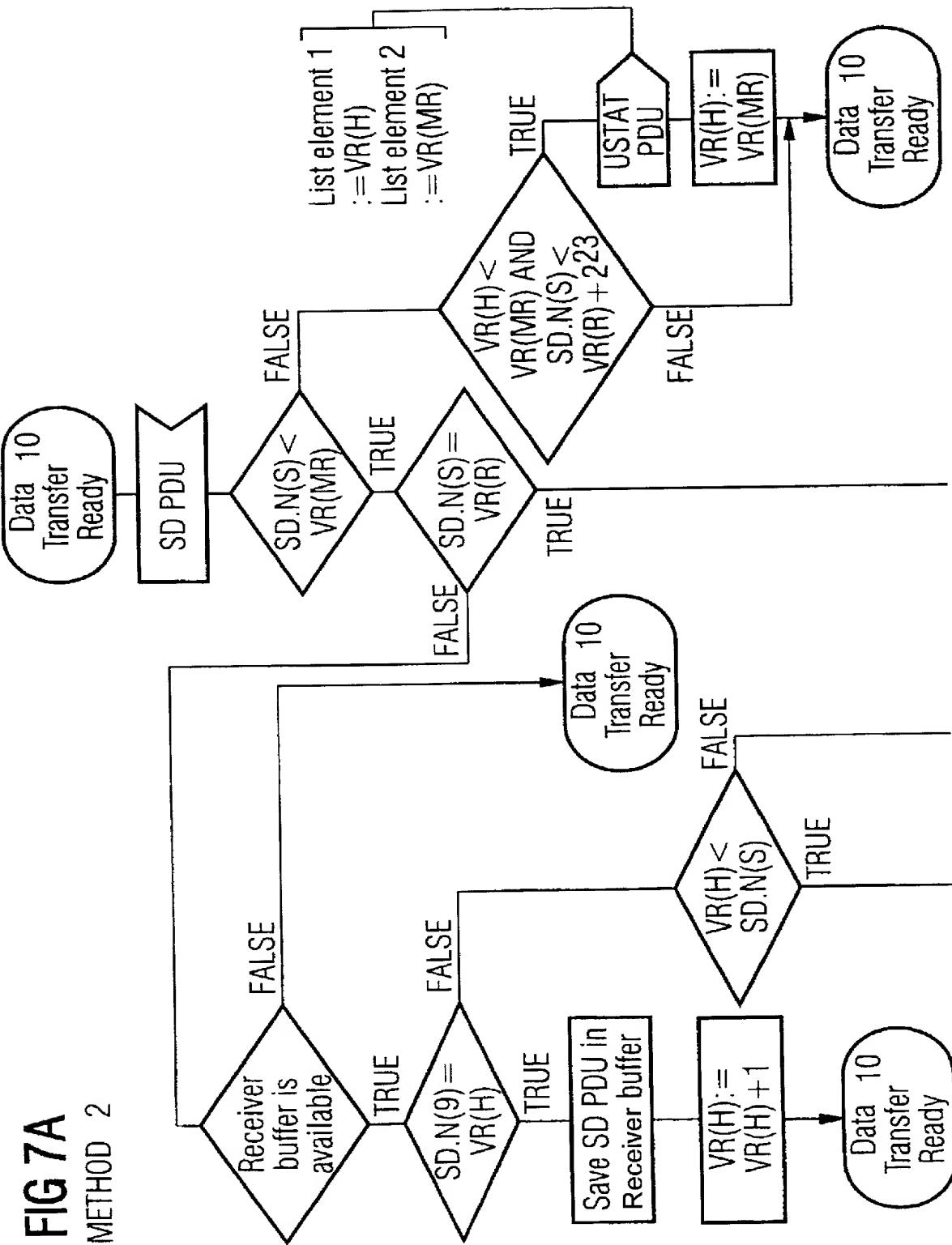


FIGURE 20 (sheet 44 of 51)
Process SSSCOP

9/11



10/11

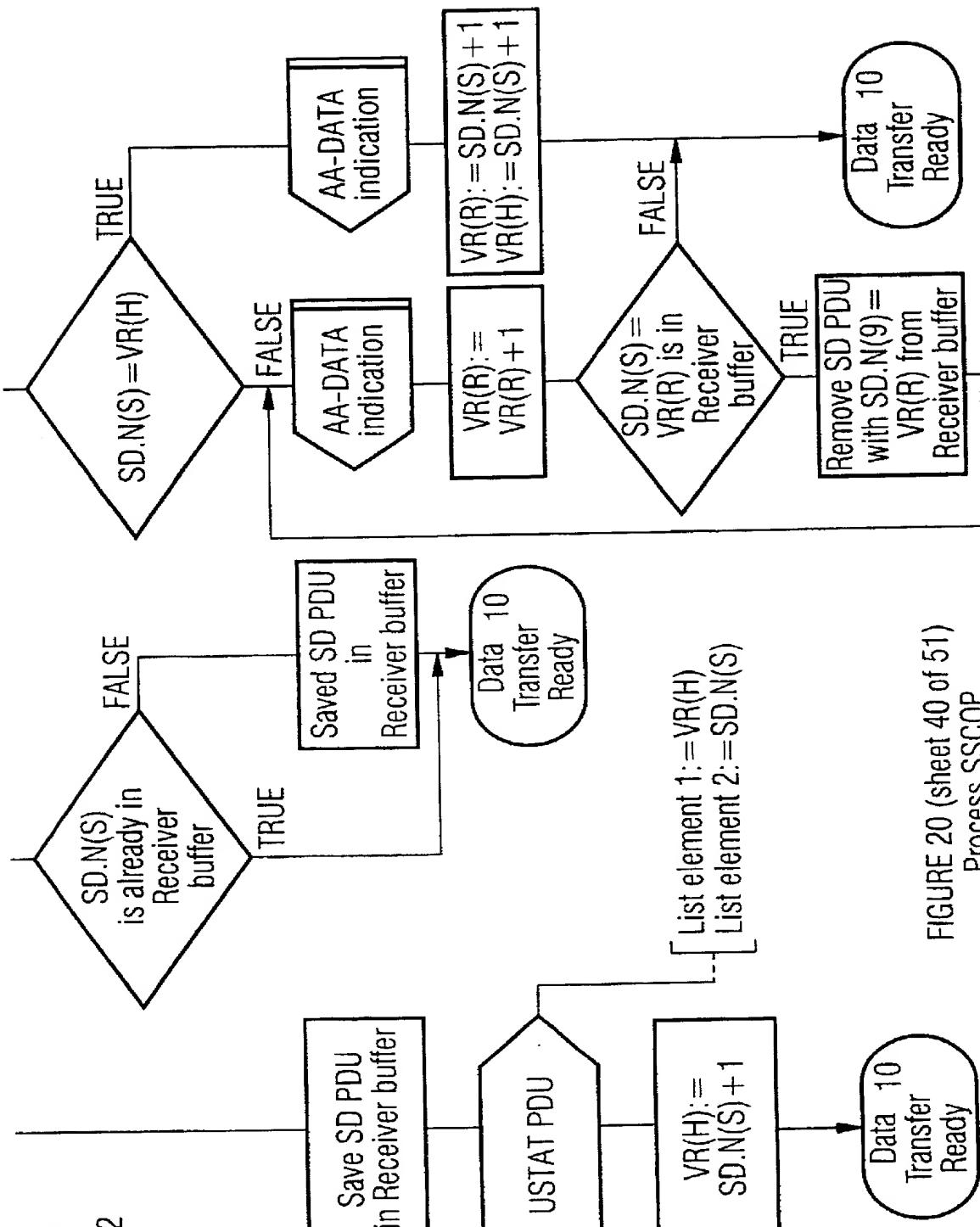
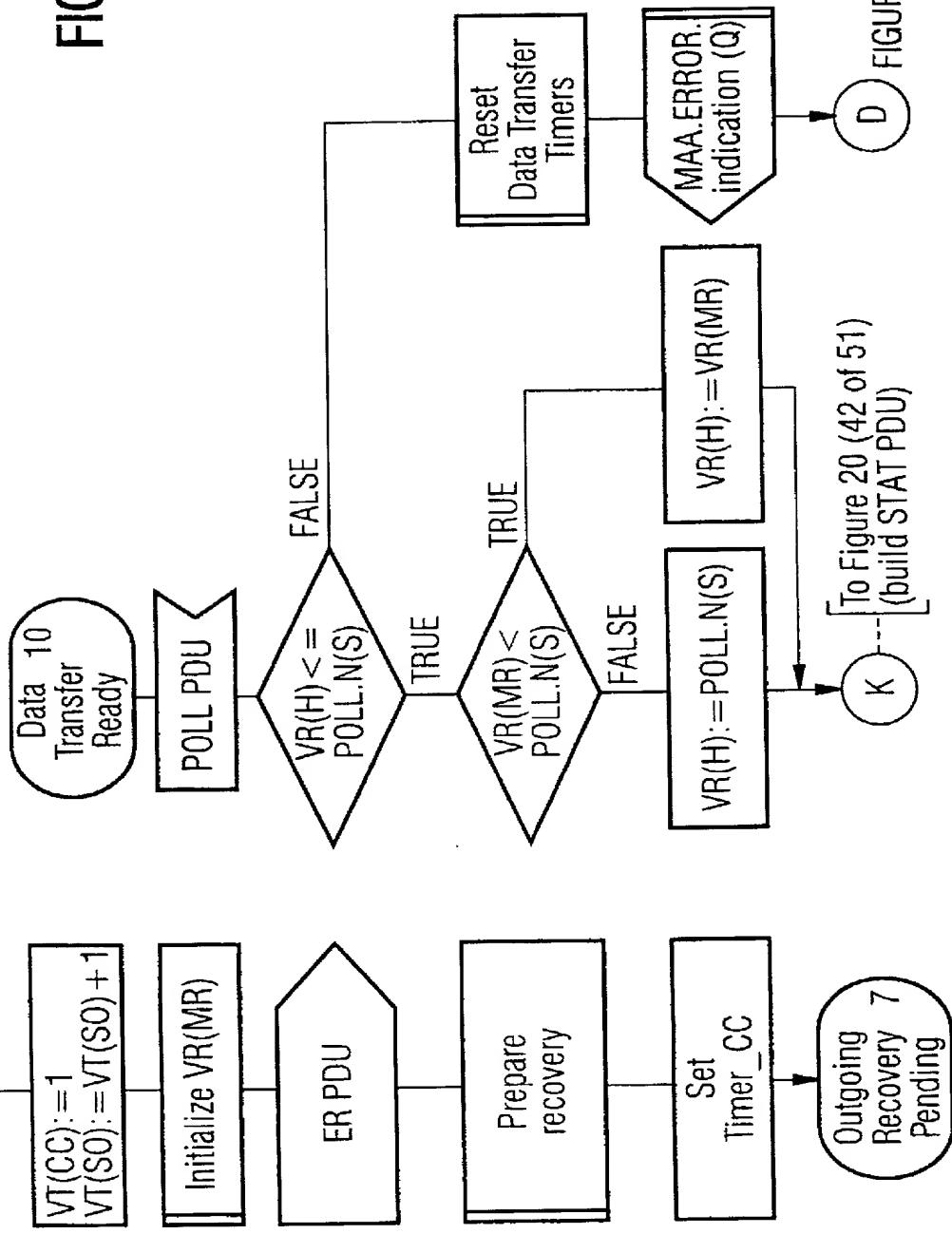


FIGURE 20 (sheet 40 of 51)
Process SSCOP

FIG 8

D [From Figure 20 (40, 41, 43 and 44 of 51)
Start error recovery procedures



D FIGURE 20 (sheet 41 of 51)
Process SSCOP

German Language Declaration

Prior foreign applications
Priorität beansprucht

Priority Claimed

198 95 6078.8 Germany 04. Dezember 1998

(Number) (Country)
(Nummer) (Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

Yes No
Ja Nein

(Number) (Country)
(Nummer) (Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

Yes No
Ja Nein

(Number) (Country)
(Nummer) (Land)

(Day Month Year Filed)
(Tag Monat Jahr eingereicht)

Yes No
Ja Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmelde datum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmelde datum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application

(Application Serial No.)
(Anmeldeseriennummer)

(Filing Date)
(Anmelde datum)

(Status)
(patentiert, anhängig,
aufgegeben)

(Status)
(patented, pending,
abandoned)

(Application Serial No.)
(Anmeldeseriennummer)

(Filing Date)
(Anmelde datum)

(Status)
(patentiert, anhängig,
aufgegeben)

(Status)
(patented, pending,
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozeßordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Declaration and Power of Attorney For Patent Application**Erklärung Für Patentanmeldungen Mit Vollmacht****German Language Declaration**

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren zur gesicherten Datenübertragung

deren Beschreibung

(zutreffendes ankreuzen)

hier beigefügt ist.

am _____ als

PCT internationale Anmeldung

PCT Anmeldungsnummer _____

Eingereicht wurde und am _____

Abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmelde-datum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

(check one)

is attached hereto

was filed on _____ as

PCT international application

PCT Application No. _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

09/857153
532 Rec'd PCT/US 31 MAY 2001

BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

CHANGE OF ADDRESS OF APPLICANTS' REPRESENTATIVE

APPLICANT(S): Klaus David GRADISCHNIG et al

ATTORNEY DOCKET NO.: P01,0183

INTERNATIONAL APPLICATION NO: PCT/EP99/09496

INTERNATIONAL FILING DATE: 04 December 1999

INVENTION: METHOD OF SECURE DATA TRANSMISSION

Assistant Commissioner for Patents,
Washington D.C. 20231

SIR:

Members of the firm of Hill & Simpson designated on the original Power of Attorney have merged into the firm of Schiff Hardin & Waite. All future correspondence for the above-referenced application therefore should be sent to the following address:

SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
CUSTOMER NUMBER 26574

Submitted by,

Mark Bergner

(Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower
Chicago, Illinois 60606-6473
Telephone: (312) 258-5779
Attorneys for Applicants
CUSTOMER NUMBER 26574

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Messrs. John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Gwynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an:
(Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

312/876-0200
Ext. _____

Postanschrift:

Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders: GRADISCHNIG, Klaus David <i>10.1.2000</i>		Full name of sole or first inventor:	
Unterschrift des Erfinders <i>Klaus David</i>		Inventor's signature	
Datum <i>10.1.2000</i>		Date	
Wohnsitz D-82131 Gauting, Germany		Residence	
Staatsangehörigkeit Bundesrepublik Deutschland		Citizenship	
Postanschrift Max-Klinger-Str. 28		Post Office Address	
D-82131 Gauting Bundesrepublik Deutschland			
Voller Name des zweiten Miterfinders (falls zutreffend): SCHWARZBAUER, Hanns		Full name of second joint inventor, if any:	
Unterschrift des Erfinders <i>Hanns Schwarzauer</i>		Second Inventor's signature	
Datum <i>10.1.2000</i>		Date	
Wohnsitz D-82194 Gröbenzell, Germany		Residence	
Staatsangehörigkeit Bundesrepublik Deutschland		Citizenship	
Postanschrift Edelweissstrasse 2A		Post Office Address	
D-82194 Gröbenzell Bundesrepublik Deutschland			

(Bitte entsprechen Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Voller Name des dritten Miterfinders:		Full name of third joint inventor.	
TÜXEN, Michael			
Unterschrift des Erfinders	Datum	Inventor's signature	Date
<i>Michael Tüx</i>	<i>10.1.2000</i>		
Wohnsitz	Residence		
D-81479 München, Germany	<i>DEK</i>		
Staatsangehörigkeit	Citizenship		
Bundesrepublik Deutschland			
Postanschrift	Post Office Address		
Gasparistr. 8			
D-81479 München			
Bundesrepublik Deutschland			
Voller Name des vierten Miterfinders (falls zutreffend):		Full name of fourth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz	Residence		
Staatsangehörigkeit	Citizenship		
Postanschrift	Post Office Address		
Voller Name des fünften Miterfinders (falls zutreffend):		Full name of fifth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz	Residence		
Staatsangehörigkeit	Citizenship		
Postanschrift	Post Office Address		
Voller Name des sechsten Miterfinders (falls zutreffend):		Full name of sixth joint inventor, if any:	
Unterschrift des Erfinders	Datum	Inventor's signature	Date
Wohnsitz	Residence		
Staatsangehörigkeit	Citizenship		
Postanschrift	Post Office Address		

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).